# Comment acheter des peluches ?

**ou petit guide d'utilisation des marchés du darknet**
**v1**

herisson

02-04-2020

Ce guide se donne pour modeste but d'expliquer au néophyte comment acheter ses peluches préférées sur le darknet. Des compétences basiques d'informatique (*i.e.* savoir allumer son ordinateur, installer un logiciel, scanner une carte d'identité) sont attendues. Il est également important de noter que ce guide est adapté pour celui ou celle qui souhaite se procurer des peluches pour sa seule utilisation personnelle ; il ne saurait servir à une personne qui a pour projet de devenir un véritable revendeur de mignonnerie en vendant des peluches à la dizaine. Il est par ailleurs destiné aux utilisateurs de Windows (je considère que les utilisateurs de Linux sont assez malins pour adapter le guide). L'auteur se décharge de toute responsabilité quant à l'utilisation de son guide pour des activités illégales. Ce document contient des liens hypertexte, ils seront soulignés.

D'autre part, il est important de garder à l'esprit que la notion d'anonymat développée au sein de ce guide est on ne peut plus relative. L'anonymat total n'existe pas. Ce guide présente un début de démarche en ce sens, mais n'est clairement pas suffisant : n'importe quelle puissance étatique un tant soit peu motivée remontera sans problème jusqu'à vous. Néanmoins, bien que cela puisse se discuter et changer au cours des prochaines années, en tant que simple consommateur de peluches, vous ne devriez avoir rien à craindre, les services de renseignement préférant dédier les ressources importantes nécessaires à un tel traçage à des cibles plus intéressantes.

# 1 Le darknet

Ce qui est communément appelé *darknet* (ou, improprement, *Deep Web*) est une partie du Web inaccessible à partir des navigateurs traditionnels. Il est accessible grâce au réseau TOR (*The Onion Router*), et en particulier du logiciel Tor Browser, et vise à garantir l'anonymat et de celui qui l'utilise. Pour une explication en détail du fonctionnement du réseau TOR, je vous invite à vous reporter à la page Wikipédia. Différents types de sites sont hébergés sur le darknet : des copies de sites existant également sur le clearnet, des services email permettant aux journalistes dans des zones sensibles de communiquer, des forums, des wikis, des moteurs de recherche, et des markets. C'est à cette dernière catégorie de sites que nous allons nous intéresser dans la suite de ce guide. Mais avant cela, attardons nous sur quelques points préliminaires.

# 2 Les cryptomonnaies

Pour acheter votre peluche, il vous faudra bien entendu un moyen de paiement. Impensable de payer par carte bancaire tout en gardant son anonymat : les markets du darknet se sont rabattus sur les cryptomonnaie.

## 2.1 Le Bitcoin

Le bitcoin (BTC) est une des premières cryptomonnaies apparues. Il est aujourd'hui très facile de s'en procurer. Plusieurs étapes pour cela :

- Téléchargez et installez un porte-monnaie électronique (*wallet*). Je recommande personnellement l'utilisation d'Electrum. Une fois installé, créez un nouveau portefeuille standard en laissant les options par défaut, la procédure est très simple. Notez bien la graine de génération du portefeuille (*seed*), elle vous servira à récupérer le portefeuille en cas de perte du fichier portefeuille. Je vous conseille de choisir un mot de passe long, et idéalement généré aléatoirement, vous pouvez pour cela utiliser des utilitaires comme KeePassX.
- Inscrivez vous sur une plateforme d'achat de cryptomonnaies. Je recommande Coinbase. Là aussi, aucune difficulté. Vous aurez besoin d'un justificatif d'identité et/ou d'un justificatif de domicile.
- Une fois votre identité vérifiée par Coinbase, vous pourrez acheter du Bitcoin. Vous pouvez approvisionner votre compte Coinbase par carte ou par virement bancaire ; le virement engendre moins de frais, mais est plus long. Je vous recommande cependant de ne s'attaquer à la conversion vers le Bitcoin qu'une fois que vous aurez choisi votre peluche, car le Bitcoin peut très rapidement perdre de sa valeur (et il serait bête de se retrouver avec une demi-peluche).

— Une fois que vous avez acheté du Bitcoin, il est stocké sur votre wallet interne Coinbase. Transférez-le vers votre portefeuille Electrum fraîchement créé. Pour cela, vous aurez besoin d'une adresse de réception : vous la trouverez dans l'onglet "Recevoir" de Electrum.

## 2.2 Le Monero (pour les plus paranoïaques d'entre nous)

Le Monero est une autre cryptomonnaie. Elle pallie un inconvénient majeur du Bitcoin. En effet, lorsqu'une transaction Bitcoin ou Monero a lieu, elle est inscrite dans une grosse base de données appelée *blockchain*. Dans le cas du Bitcoin, l'adresse de l'émetteur et du récepteur font partie des informations inscrites dans la *blockchain*, visible par tous, on peut donc, avec des algorithmes créés pour, suivre les déplacements de Bitcoin d'adresse en adresse, pour potentiellement remonter jusqu'à la plateforme d'achat, et la forcer à révéler votre identité ! Dans le cas d'une transaction Monero, les adresses de l'émetteur et du récepteur ne sont pas inscrites dans la *blockchain*, ce qui empêche ce genre de problème. D'autre part, certains markets ne permettent d'utiliser que le Monero.

Pour obtenir du Monero, la marche à suivre est très similaire :

— Créer un wallet. Electrum ne gère que le Bitcoin, je conseille donc le wallet officiel (*GUI Wallet*) de Monero. Lors de la création, mêmes recommandations : choisissez *Simple Mode*, laissez les options par défaut, prenez un mot de passe long, notez bien la seed.

— Pour acheter du Monero, vous avez deux options :

  — Convertir du Bitcoin acheté comme expliqué précédemment en Monero, pour cela je conseille le très bon site MorphToken.

  — Acheter directement du Monero, mais les plateformes d'échange qui le proposent sont plus rares. Je conseille Kraken.

— Si vous souhaitez utiliser du Monero pour son anonymat, mais le market où vous achetez vos peluches ne prend que le Bitcoin (honte à lui), il existe le service xmr.to : on lui envoie du Monero, et il se charge d'envoyer du Bitcoin au market en échange, dans le plus grand des anonymats.

# 3 PGP

À un moment donné, il vous faudra envoyer votre adresse à votre vendeur, afin que celui-ci sache où expédier votre peluche ; il est cependant impensable de l'envoyer "en clair", si jamais le market se fait pirater, ou ses serveurs se font saisir, tout le monde saurait que vous achetez des peluches ! Il est donc nécessaire de chiffrer (et non de crypter, qui est un anglicisme, *cf.* chiffrer.info) ce genre de messages sensibles. Pour ce faire, on utilise le standard OpenPGP (Pretty Good Privacy), et plus particulièrement son implémentation GPG. Il permet un chiffrement asymétrique des données. Sans rentrer dans les détails, ce qu'il y a à savoir sur le chiffrement asymétrique :

- Un utilisateur de GPG génère d'abord une paire de clés. Chaque paire de clés est constituée d'une clé "publique" et d'une clé "privée"
- Soient deux utilisateurs, Alice et Bob. Si Alice veut envoyer un message privé à Bob, elle devra le chiffrer avec la clé publique de Bob, l'envoyer à Bob, puis Bob pourra le déchiffrer grâce à sa clé privée. On comprend bien ici les appellations "clé publique" et "clé privée" : autant il est important pour Bob de diffuser sa clé publique pour qu'on puisse lui envoyer des messages chiffrés, autant il ne faut surtout pas qu'il diffuse sa clé privée, car c'est elle qui lui permet de déchiffrer les messages qu'il reçoit.
- De la même manière, si Bob souhaite envoyer un message à Alice, il faudra qu'il lui demande sa clé publique, qu'il chiffre son message avec, le lui envoie, et qu'Alice le déchiffre grâce à sa clé privée.
- Autre cas de figure. Alice veut envoyer un message à Bob, pas spécialement sensible, disons l'heure et le lieu à laquelle ils doivent se retrouver pour manger ensemble. Mais comment Bob peut savoir que c'est bien Alice qui lui a envoyé ce message, et pas Charlie qui veut lui tendre un piège ? Pour ce faire, Alice peut *signer* son message grâce à sa clé privée, et à la réception Bob pourra le vérifier grâce à la clé publique d'Alice. Comme la signature dépend du contenu du message, et seule Alice possède sa clé privée, personne d'autre ne pourra générer une signature qui soit vérifiable par la clé publique d'Alice.

Pour en savoir plus sur OpenPGP et le chiffrement asymétrique, je vous renvoie vers les pages wikipédia de PGP et de RSA

Regardons maintenant comment cela fonctionne en pratique. Sur Windows, gpg n'est pas inclus dans le système d'exploitation, il faut donc télécharger la version de gpg pour windows, appelée Gpg4win. Une fois le téléchargement effectué (on choisira de donner 0$ si on est radin), vous pouvez décocher toutes les cases sauf GnuPG dans l'assistant d'installation, et installer. Pour utiliser GPG, lancez l'invite de commandes Windows en appuyant sur les touches `Win + R`, en écrivant `cmd` en face de "Ouvrir :" et en cliquant sur OK. Une fois l'invite de commande lancée, vous pouvez utiliser GPG dedans.

Notez bien que le dossier dans lequel vous vous trouvez par défaut est votre dossier utilisateur (`C:\Users\VOTRENOMDUTILISATEUR`), si vous souhaitez travailler dans un autre dossier, vous pouvez utiliser la commande `cd` de la façon suivante :

```
cd C:\Users\herisson\Desktop
```

pour se déplacer sur le Bureau par exemple (il suffit de taper la commande dans la console et d'appuyer sur Entrée). Le dossier dans lequel vous vous trouvez est indiqué au début de la ligne. Une fois que vous vous êtes placés dans le dossier de votre choix, vous pouvez exécuter toutes les commandes gpg utiles. Par ailleurs, pour copîer du texte affiché dans une console, sélectionnez le texte à copier, puis effectuez un simple clic droit dessus ; pour coller du texte, un simple clic droit n'importe où dans la console suffit.

Je vous recommande de créer et d'éditer tous les fichiers texte dont vous pourrez avoir besoin avec le Bloc-Notes Windows (et bien entendu de les enregistrer dans votre dossier de travail).

Voici les commandes dont vous aurez besoin :

— `gpg --generate-key` : pour générer une paire de clés. Vous n'aurez besoin de l'exécuter qu'une seule fois. Vous pouvez mettre n'importe quoi dans "Nom Réel" et "Adresse e-mail", c'est juste pour identifier votre paire de clés (mais les gens avec qui vous correspondrez les verront). Même conseil que d'habitude pour la phrase secrète : quelque chose de long.

— `gpg --import key.txt` : pour importer la clé publique de quelqu'un avec qui vous souhaitez correspondre. `key.txt` est un fichier texte dans votre dossier de travail contenant la clé publique.

— `gpg -k` : pour lister les clés publiques importées

— `gpg -K` : pour lister les clés privées (au cas où ça vous prendrait d'avoir plusieurs identités)

— `gpg --export -a NOM` : pour afficher la clé publique associée à `NOM` (utiliser `gpg -k` pour savoir le nom à utiliser)

— `gpg -ase -u NOM DE L'EMETTEUR -r NOM DU RECEPTEUR message.txt` : pour chiffrer et signer le message contenu dans le fichier `message.txt` dans le dossier de travail. Cette commande crée un fichier `message.txt.asc` contenant le message chiffré. Les noms du récepteur et de l'émetteur sont ceux qui apparaissent dans `gpg -k` et `gpg -K`

— `gpg --clear-sign -u NOM DE L'EMETTEUR message.txt` : pour signer sans chiffrer le message contenu dans le fichier `message.txt` dans le dossier de travail. Cette commande crée un fichier `message.txt.asc` contenant le message signé. Vous n'en aurez pas besoin pour des cas basiques d'utilisation de gpg dans le cadre d'achats sur le darknet.

— `gpg --decrypt messageChiffre.txt` : pour déchiffrer le message contenu dans le fichier `messageChiffre.txt` dans le dossier de travail ; le message déchiffré s'affiche dans la console.

— `gpg --verify messageSigne.txt` : pour vérifier un message signé (il faut importer la clé publique correspondante avant). Le résultat de la vérification s'affiche dans la console.

# 4 Commandons notre peluche !

## 4.1 Installation de Tor Browser et premiers pas

Rentrons maintenant dans le vif du sujet. Commencez par installer Tor Browser, et lancez-le. Cliquez sur "Connect", et après quelques secondes, vous avez une belle fenêtre qui s'affiche : félicitations, vous pouvez aller sur le Darknet !

Avant d'aller plus loin, vérifiez que le petit bouclier à droite de la barre d'adresse est bien entièrement noir ; sinon cliquez dessus, puis sur "Advanced Security Settings", et réglez le niveau de sécurité sur "Safest". Ensuite, nous allons mettre le site `dark.fail` en page d'accueil. Ce site, géré par un journaliste, répertorie la grande majorité des sites du darknet considérés comme fiables. Saisissez l'URL `dark.fail` dans la barre d'adresse. Copiez l'URL en `.onion` citée en début de site ; au jour où j'écris ces lignes, cette url est `darkfailllnkf4vf.onion`. Allez dans le menu de Tor Browser en haut à droite (trois barres horizontales), puis dans Options, Home (dans la colonne de gauche), choisissez "Custom URLs" en face de "Homepage and new windows", et collez l'URL que vous avez copiée dans le champ de texte. Et voilà !

Les URL en `.onion` comme celle que vous venez de copier sont des URL de sites du réseau TOR, elles ne marcheront pas sur des navigateurs ordinaires. En navigant sur le darknet, il est toujours conseillé de copier-coller les URL plutôt que de cliquer dessus (elles ne seront d'ailleurs en général pas cliquables).

## 4.2 Choix du market

Maintenant, lorsque vous lancez Tor Browser, vous atterissez sur le site de `dark.fail` sur le darknet. Vous pouvez choisir le market qui vous plaît dessus. Prenez l'habitude de toujours piocher les liens sur `dark.fail`, même lorsque vous trouvez une URL autre part ; si le site est listé sur `dark.fail`, prenez l'URL dessus. Vous trouverez notamment dessus un lien vers Dread, l'équivalent darknet de Reddit, qui vous servira à chercher des avis sur les différents markets et vendeurs, ou vers des agrégateurs de markets comme Kilos ou Recon.

Vous pouvez maintenant choisir un market. À noter que pour accéder aux peluches vendues sur un market, il est presque toujours nécessaire de s'inscrire sur celui-ci. À l'inscription, on vous demandera sûrement votre clé PGP, et vous serez fier de la copier-coller grâce à un petit `gpg --export VOTRENOM` !

## 4.3 Choix de la peluche

Pour choisir votre peluche, rien de plus simple ! Il suffit d'utiliser les fonctions de recherche des markets. Quelques conseils :

— Je vous recommande de sélectionner la catégorie de la peluche que vous souhaitez dans la liste déroulante des catégories plutôt que de taper ladite catégorie dans la barre de recherche.

— Cherchez des peluches envoyées de France à France (ou de Suisse à Suisse, ou de Belgique à Belgique, vous avez saisi l'idée), en effet, il est bien connu que les douaniers veulent empêcher les citoyens de profiter de la mignonnerie d'une douce peluche, alors autant éviter que le colis passe dans leur mains ! Au niveau national, il est extrêmement rare que la poste ouvre un colis.
— Une fois que vous avez repéré plusieurs produits qui vous conviennent par les photos, le prix etc., regardez un peu le profil des vendeurs. Commencez par les reviews du vendeur, tout en gardant en tête que des reviews positives pourraient être rajoutées par le vendeur lui-même, et que des reviews négatives pourraient être rajoutés par des concurrents.
— N'hésitez pas à chercher des reviews du même vendeur sur d'autre markets, ou bien sur des sites externes comme Dread ou Recon.
— Faire attention si la peluche sélectionnée est en paiement "Escrow" ou "Finalize Early". "Escrow" signifie que votre argent passe par un intermédiaire, généralement le market lui-même, et n'est relâché au vendeur que lorsque vous confirmez avoir reçu la commande. Si vous ne recevez rien au bout de x jours (délai dépendant des markets) vous pouvez ouvrir une "dispute" avec le vendeur pour lui demander ce qu'il en est de votre commande. "Finalize Early", au contraire, vous oblige à envoyer votre argent dès le placement de votre commande, ce cas n'est donc à utiliser qu'en cas de grande confiance accordée au vendeur, ce qui n'arrive *de facto* jamais sur le darknet.
— Les *Trust Level* qui sont parfois présents sur des markets ne sont pas du tout représentatifs de la véritable confiance que l'on peut accorder à un vendeur ; la manière dont ce Level augmente est assez floue, il est parfois acheté, bref, ne pas s'y fier.
— Les vendeurs qui disent "nous on n'utilise pas PGP, ça fait perdre du temps", c'est out direct, sans réfléchir.
— Une fois qu'un ou plusieurs vendeurs vous ont définitivement convaincus, je conseille de leur envoyer un petit message privé demandant des détails sur la peluche, comment ils l'envoient, s'ils la mettent sous vide etc. Même si on s'en fout ou que tout est relativement clair dans la description de la peluche, cela permet de voir s'ils sont réactifs, comment ils répondent, etc. Ils peuvent même envoyer un lien vers leur market privé s'ils en ont, où les frais seront moindres. Si vous ne recevez pas de réponse dans un temps acceptable (2-3 jours), je vous conseille de ne pas poursuivre avec ce vendeur.

### 4.4 Le moment de la commande

Maintenant que vous avez choisi la peluche que vous souhaitez prendre, on passe à la commande ! C'est là que vont nous servir les deux paragraphes introductifs. Le passage de la commande se fait assez intuitivement et facilement, à part peut-être deux étapes sur lesquelles il est intéressant de revenir :

— L'envoi de l'adresse : À un moment dans le passage de la commande, on vous demandera d'écrire votre adresse : c'est là qu'il faudra chiffrer le message ; on commence par importer la clé PGP publique du vendeur disponible sur son profil, puis on chiffre son message grâce à la commande `gpg` dédiée. Ne pas faire confiance aux petites cases à cocher "chiffrer ce message" parfois présentes sur les markets, toujours chiffrer soi-même ses messages.
— Le paiement : certains markets envoient l'adresse sur laquelle transférer l'argent au moment de la commande, d'autres demandent d'approvisionner un wallet interne avant de placer une commande. Dans les deux cas, cela se fait facilement avec l'onglet "Envoyer"/"Send" d'Electrum ou de Monero Wallet. Petite subtilité lors de l'envoi de Bitcoin : on peut régler un "frais de transaction", cela concerne le mécanisme interne de confirmation des transactions, plus le frais qu'on met sur la transaction est élevé, plus elle sera confirmée vite (la confirmation est nécessaire pour la prise en compte de la transaction par le market)

## 5 Fin

Bravo, vous avez réussi à commander votre peluche préférée ! Je vous souhaite bonne réception de celle-ci, et plein de câlins trop mignons ☺

Pour toute question, suggestion ou réclamation sur ce guide, je vous remercie d'écrire un email à l'adresse : `herisson@cock.li`

Ce document est mis à disposition selon les termes de la licence Creative Commons “Attribution - Pas d'utilisation commerciale - Partage dans les mêmes conditions 4.0 International”.